Microsoft Exchange Server

Chapter 6.1
Exchange 2000 Security and Administrative Models

Planning Guide

Abstract

This chapter outlines the changes in the administrative model that will become apparent when you migrate to Exchange 2000. After completing these steps, you will be able to implement an administrative model and security model that will fit your organizational requirements.

This is a preview edition of the Microsoft Exchange 2000 Server Upgrade Series. The final documentation will be available in November 2000.

© 2000 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

1000

CONTENTS

INTRODUCTION....1
Design Considerations 1
Resource Requirements 1
System Prerequisites 1

BUILDING THE SECURITY MODEL....2
What You Will Need 2
What You Should Know 2
Determine Security Requirements 2
Exchange 5.5 Security Model Review 2
Exchange 5.5 Journaling Requirements 4
Exchange 2000 Journaling Capabilities 4
Exchange 5.5 Administrative Tool Restrictions 4
Exchange 2000 Security Capabilities and Requirements 4
Exchange 2000 Administrative Tools – MMC 6
Exchange 2000 Security Model Design 6

BUILDING THE ADMINISTRATIVE MODEL....7
Design Considerations 7
User Administration 8
Server Management 8
Routing 9
Public Folders 9

Summary....10

INTRODUCTION

This chapter will help you design your Exchange 2000 security and administrative models, using both your current system and your requirements as templates. When implemented, these models will allow your users to perceive only differences where the new implementation, based on your requirements, differs from the current implementation.

One thing you will encounter as you design these models is that the models will influence each other. For example, you may be able to simplify the way you administer your environment with Exchange 2000 in ways that you did not expect when you built your security model. You may then need to revisit the security model and update it to reflect the changes in the administrative model. This guide discusses the models in a logical order, the security model supporting the administrative model. As you work with the models, you should consider them living documents that will be updated throughout your planning process.

Design Considerations

This section will try to help you deal with the politics of your organization when you build your administrative and security models. It will also show you that if you have implemented certain Exchange 5.5 capabilities, you will be able to cleanly upgrade to Exchange 2000 without interrupting their operation.

For both administrative and security requirements, Exchange 2000 provides the technology to solve an organization’s political requirements. Therefore, the technologies will be discussed as you encounter them in the process.

Resource Requirements

As the current Exchange administrator, you will be leading the security and administrative design sessions. However, since Exchange 2000 relies on Windows 2000 for its security, and for some of its administrative control, you will need to include your organization’s Active Directory administrators in your planning cycle. Additionally, if you are the system architect, you will need to include your organization’s operational system administrators as well.

System Prerequisites

Before reading this chapter, you should have determined which Exchange 2000 technologies you wish to implement, found all your system dependencies, and completed your Windows 2000 Active Directory design. If you have not completed any of these three areas, you may wish to read the earlier chapters in this guide before continuing.

BUILDING THE SECURITY MODEL

As with any messaging application implementation, you will require a security structure that restricts who has access to different parts of your messaging system. You can use combinations of auditing, permissions, and restrictions in various areas of the system to ensure that your users are not hampered in their daily use, but that when they try to bend the rules, at the very least you know who has been doing what. With whom. And when. You may want to, for example, implement journaling on some or all of your mailboxes to ensure that you have copies of all messaging traffic from particular mailboxes.

What You Will Need

To carry out the planning in this chapter you will require the following:

- Documentation on your current Exchange security design.
- Documentation on your current Windows 2000 security design.
- Documentation on your current network security design.

What You Should Know

You should also know certain information:

- External information that will influence your security design – these include legal regulations and requirements.
- Requirements that were not implemented as part of your current Exchange design.

Once you have this data, you can proceed with your planning.

Determine Security Requirements

Before designing your security infrastructure for Exchange 2000, you should review your security requirements. Your Exchange 5.5 security model will be used as a starting point, but since Exchange 2000 uses Windows 2000 as its security provider, there will be differences.

Exchange 5.5 Security Model Review

Exchange 5.5 security models were driven by two requirements:

- Security requirements on the various aspects of your Exchange system.
- Integrating security into your Exchange site topology.

To secure various aspects of your Exchange system, which was truly driven by your security requirements, you granted specific Exchange rights to portions of the Exchange organization. To do this with Exchange 5.5, you had to grant permissions to either Exchange mailboxes or

Windows accounts depending on what kind of resource you were securing.

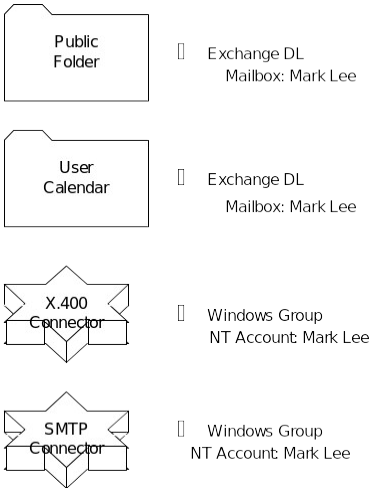

Figure 1. Placing Permissions in Exchange 5.5

For example, if you needed to be sure that certain public folders or users' calendars were only available to specific users, for the folder access permissions, you used Exchange mailboxes to grant permissions. If you wanted to be sure that an SMTP or X.400 connector could be viewed, but not modified, by a group of individuals, you used Windows NT accounts. This meant that you might have to grant permissions to both a mailbox and an account so that a single person would be able to administer your Exchange system. (You can use Windows groups and Exchange distribution lists to ease this administrative burden, but it is still a two-level administrative process.)

After this level of security, you had another level, where you had to expand your security considerations because you had multiple Exchange 5.5 sites in your organization. This meant that if you needed to be able to modify parts of the Exchange system in remote sites, you had to be sure you had rights to that part of the Exchange system. This required you to have rights granted at both the Exchange level and the Windows NT level.

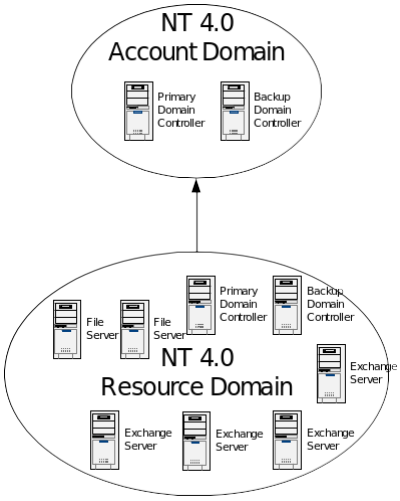

Figure 2. Exchange 5.5 Trust Requirements

For example, if you have a user account in the Windows NT 4.0 accounts domain, and you needed to administer Exchange servers in the organization's resource domain, you had to have Exchange admin rights, and you had to be sure that the resource domain trusted the accounts domain.

The combination of these two levels of security could cause a large organization to have a complex security environment, even if they had relatively few people with administrative rights.

Once you have reviewed your current Exchange 5.5 security model, you are going to determine if these correspond to your organizational requirements.

Exchange 5.5 Journaling Requirements

Many government organizations have a security requirement to keep copies of all messaging traffic that goes through their electronic messaging system, and have built elaborate add-ons to their older messaging systems so they could address these needs. This functionality allows a messaging administrator to determine if corporate or organizational information is being transmitted to other parties with minimal effect on the users and their mailboxes.

With Exchange 5.5, Microsoft included this functionality in the product. Many of our customers built systems with this capability and require the same features in any upgrade.

Exchange 2000 Journaling Capabilities

Just like Exchange 5.5, Exchange 2000 offers journaling features for monitoring messaging traffic. If you are currently using journaling in your Exchange 5.5 organization, you will still have this functionality when you upgrade to Exchange 2000.

Exchange 5.5 Administrative Tool Restrictions

With all previous versions of Exchange, most administrative tasks were done from the Exchange Administrator console. To use this tool, a person needed a minimum of View Only Admin permissions at the Organizational and Site level. This meant that even if the person only needed to administer an individual recipient container, the additional organizational permission was required. Although this is a view-only permission, a person with enough knowledge of the Exchange system might be able to use the knowledge of the organization and sites to their advantage.

Exchange 2000 Security Capabilities and Requirements

Since Exchange 2000 relies on Windows 2000 for applying permissions to the system, in Exchange 2000 there is only a single level of permissions to consider. For example, in the above discussion, you would configure both the public folder permissions and the connector permissions using Windows 2000 accounts or groups.

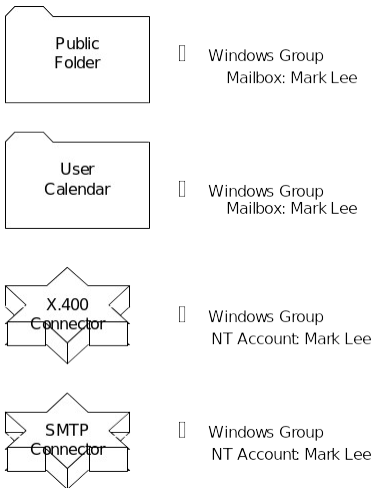

Figure 3. Placing Permissions in Exchange 2000

This makes it much easier to configure permissions, document the permissions that have been granted, and explain the permissions to other administrators or security personnel.

At the Exchange site level, since Exchange 2000 can only be installed in a Windows 2000 environment, cross-domain trust issues are a moot point. However, if your organization has a Windows NT 4.0 domain environment that is being replaced by a Windows 2000 environment, you may have more trust issues than before. The cleanest security structure may be one where you have two-way trusts between all domains that are hosting your Exchange 2000 servers and your Exchange 5.5 servers, and you can then add trusts between your Windows NT 4.0 account domains and your Exchange 2000 servers as necessary.

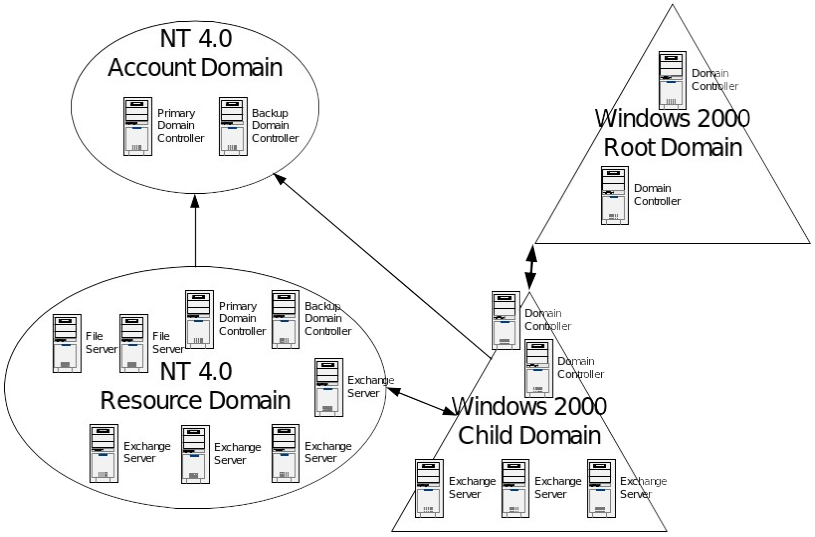

Figure 4. Exchange 2000 Trust Requirements

The result of this discussion is that even though Exchange 2000 can reduce the complexity of granting permissions in your Exchange system at the object level, it may cause a more complex arrangement if you must co-exist with Exchange 5.5 and Windows NT 4.0. As you design your Exchange 2000 security model, you need to be aware of the implications of co-existence.

Exchange 2000 Administrative Tools – MMC

Unlike Exchange 5.5, Exchange 2000 administrators use Microsoft Management Console (MMC) to administer the system. For mailbox management, administrators will use the Windows 2000 Active Directory Users and Computers Snap-in, and for Exchange configuration management, they will use the Exchange 2000 System Manager Snap-in. Each of these is fully configurable; therefore, if a mailbox administrator only needs access to a single Windows 2000 OU, that administrator's level of authority can be confined to that OU without having access to any other part of the system. Additionally, you can build the sandboxed Snap-in configurations and deliver them to administrators who do not require access to the entire system. This provides a great amount of flexibility in setting the permissions that any single person has over your system.

Exchange 2000 Security Model Design

Working from the information that you have gathered from your Exchange organization and the additional security requirements for your physical organization, you can now design your Exchange 2000 security model. If you are designing your architecture for co-existence between Exchange 5.5 and Exchange 2000, while you will reduce the complexity

of your permissions, you will increase the number of Windows trusts you need to maintain. As stated above, this is required to allow mixed Exchange systems to function properly.

Once you have mirrored your current environment as much as possible, you will need to expand your design to include other requirements your system will have to satisfy. These may be requirements that were not implemented in your current system because the requirements are newer than the current system, they may be requirements that the current system was not capable of, or they may be requirements that were too complex to implement in the previous version of Exchange.

Exchange 2000 supports a more granular administrative model than did Exchange 5.5. Under Exchange 5.5, giving someone the ability to manage a site gave that person the authority to manage all of the servers in a site, as well as the messaging connectors for that site. Since Exchange 2000 separates managing the servers from managing the connector objects through the concept of Administrative Groups and Routing Groups, it is possible to give these functions to different administrators. However, since Exchange no longer maintains its own directory, coordinating Exchange administration with Active Directory administration is a must.

Before designing a new administrative structure, you first have to identify the current administrative roles and functions. Create a list of people that currently are involved in the Exchange 5.5 administration process and the responsibilities/rights that those administrators have. Even if the current model works well, this would be a good time to take a look at the new administrative features of Exchange 2000, since current administrative models may have been based on the limitations of Exchange 5.5.

Design Considerations

There are several broad categories of Exchange administration that you must consider when designing the administrative model. Note that these functions are not necessarily mutually exclusive (that is, it is possible for someone to administer both users and servers). Also, each of the broad categories can be further broken down into smaller areas of authority:

- **User Administration**: Administering mailboxes in Exchange 5.5 was a separate function from managing user accounts. Now that mailboxes are an attribute of a Windows 2000 user account, mailbox administration will be closely tied to Active Directory account administration. This function might also include managing recipient policies and Global Address Lists.

- **Server Management**: Managing the Exchange servers could include: managing permissions, protocols, Exchange system policies, storage groups, and databases. Because of the new Administration Groups concept, applying a standard level of permissions across several servers is quite easy. Permissions can be set on a more granular level if that type of control is required.
- **Routing**: In large organizations, messaging paths and available routes can become complex. By allowing someone permission to manage a routing group, that administrator can control messaging connectivity for that group of servers. Note that routing groups are only available in Native Mode Exchange Organizations.
- **Public Folders**: Public folder hierarchies can become large and challenging to administer. It is a good idea to designate a person to manage public folders and folder replication. It can be beneficial to have individuals administer each public folder tree, when there are many trees to manage.
- **Collaboration**: Although not specifically covered in this document, separate administrative groups may be required to administer conferencing, instant messaging, or other collaborative services due to their specialized nature.

It is also necessary to consider the people that will be required to administer these areas.

User Administration

One common question that often arises when it comes to mailbox administration under Exchange 2000 is, “Should the administrators of Exchange also have the ability to create user accounts?” This must be determined on an individual organization basis. However, one advantage of giving the administrator this ability is that the Exchange administrators will not need to coordinate with the Active Directory administrators for basic maintenance issues.

If security of user accounts is a major concern, Exchange administrators do not need to have full control over user accounts. Administering user mailboxes requires that the administrator have the ability at least to modify the private and public information property sets for the user accounts in question. To be able to administer all the mailboxes required, it may be necessary to delegate authority for multiple organizational units. To alleviate this, Exchange administration should be a contributing factor to the initial Active Directory design.

Besides needing someone to manage the recipients themselves, you will also need someone to administer the recipient policies and Address Lists. Depending on the level of granularity desired, this could be the same person or multiple people.

Recipient policies allow the administrator to modify quickly the addressing information for a given group of people. This will be especially important in times of company mergers or dissolutions, and provides a much easier method for modifying addresses than does Exchange 5.5. You should give this role to someone that understands address spaces and connectors.

Address Lists allow users to see easily a list of available recipients in order to simplify sending messages. Address Lists also provide a measure of security, by filtering the available addresses that a user is aware of in their mail client. This is especially important in a hosted situation. An administrator that understands the needs of the users and the security requirements of the organization should manage these.

Server Management

By grouping servers into Administration Groups, you can grant several people the right to administer a group of servers easily. There are many aspects to managing Exchange servers, though, so it may be useful to further delegate permissions over smaller components of the administration groups, especially in large environments. Backing up and restoring the server, managing system policies, and managing protocols are all requirements of server management.

Maintenance of the Exchange databases is perhaps the most important aspect of server management. These must be backed up regularly to help prevent irrecoverable data loss. The person(s) responsible for database maintenance should be clearly defined to ensure that this is taken care of. Although many organizations will use automated backup systems, these administrators will be responsible for seeing that the backups take place and that a policy for testing those backups and for performing trial restores is in place.

Since Exchange 2000 uses the concept of storage groups, it is possible to make people responsible for different sets of databases, which can be vital in the case of an Exchange server that hosts mailboxes from several different companies.

Protocol management is another important concern. The admin will have the authority to control message sizes, protocol availability (that is, restricting the people that are permitted to access Exchange through a web browser), as well as view and flush message queues.

Administrators with the ability to modify Exchange System Policy will be responsible for managing logging, message tracking, database maintenance, mailbox and database limits, and indexing, to name a few. System policies will have a significant impact on the operation and maintenance of the Exchange servers, so this person must be knowledgeable in almost all aspects of Exchange.

SUMMARY

Routing

In Exchange 5.5, it was difficult to separate the concept of message routing from the Exchange Site boundary. In Exchange 2000, routing groups have been implemented to make this possible. Administration of the connectivity of groups of servers is no longer dependent on the sites that they are in.

The group of people that are responsible for message routing should have knowledge of the different types of connectors and their uses, as well as the underlying physical structure of the network. This will allow them to choose the most efficient messaging paths for the organization.

Public Folders

Public folder trees can become large and can contain a great deal of information. The person responsible for the folders should be able to create them, map them to database stores, and configure replication to ensure full time availability.

Once you have completed your draft Exchange 2000 security model, you will be able to start designing your Exchange 2000 administrative model.

If you have completed the steps in this chapter, you now have both a security model and an administrative model that fits your organizational requirements. Additionally, since you have modified the one while you designed the other, each will complement the other in your production system.

Your next step is to actually start deploying Exchange 2000 in your organization. The first step in this process is preparing your Windows 2000 organization for your first Exchange 2000 server. This is discussed in “Deploying a Microsoft Exchange 2000 Server Upgrade.”